

IN THE DRAWINGS

Formal drawings are supplied herewith.

REMARKS

This responds to the Office Action mailed on September 8, 2005, and the references cited therewith.

Claims 4, 5, 7, 8 and 20 are amended, claim 6 is canceled, claims 1-3, 14 and 15 are withdrawn from consideration, and new claims 21-34 are added; as a result, claims 4, 5, 7-13 and 16-34 are now pending in this application.

Affirmation of Election

As provisionally elected by Applicant's representative, Thomas Brennan, on August 29, 2005, Applicant elects to prosecute the invention of Group II-a, claims 4-13 and 16-20. Applicant acquiesces to the Examiner's characterization of claims 4-9 and 16-20 as generic to Group II and claims 11-13 as directed to Group II-a. In addition, Applicant submits that claim 10 is generic to Group II as well.

New claims 21-34 include claims 21, 23, 28, and 30 that are generic to Group II and claims 22, 24-27, 29 and 31-34 are directed to Group II-a.

§112 Rejection of the Claims

Claims 16-17 were rejected under 35 U.S.C. § 112, first paragraph, as failing to comply with the enablement requirement.

Claims 16-17 and 20 were rejected under 35 U.S.C. § 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention. Claim 20 has been amended to eliminate the "such as" language.

The term "fixed complex code" used in claims 16 and 17 is defined at p. 5, line 22 as a code similar to what is used in PKI. This definition is underscored by the comparison of "fixed complex code" to "fixed simple codes", "one-time codes" and "complex, one-time codes" from p. 5, line 19 through p. 6, line 8.

Reconsideration is respectfully requested.

§102 Rejection of the Claims

Claims 4-12 and 18-20 were rejected under 35 U.S.C. § 102(b) for anticipation by "RSA Web Security Portfolio - How RSA SecurID Agents Can Secure your Website" by RSA Security, Inc. (RSA).

RSA describes a two factor authentication system in which a user enters a secret personal identification number (PIN) and a one-time password generated by a token. As noted in the first paragraph of p. 2, two factor authentication is more secure than a simple static password since it relies on two independent factors. In the system described in RSA two factor authentication is based on something the user knows (the secret pin) and something the user has (a token that generates a one-time password at predetermined intervals).

The Examiner stated that RSA describes "enabling the communication of at least some of the authentication data from the first web site to a second web site using the internet" as required by claim 4. Applicant respectfully disagrees. RSA states that two factor authentication based on the PIN and the one-time password is performed in only one RSA ACE/Server. That server returns a cookie to the user that can be used to access content protected by the server. As noted on p. 3, paragraph 4, it is possible to configure the RSA ACE/Agents to communicate with each other such that the same cookie can be used to access content on two or more servers. "To do this, cookies are issued that are valid on multiple servers in the same Web domain or across multiple domains."

In contrast, Applicant teaches, and claims in claims 4, 5, 7-13 and 16-34, authenticating the user to two different web sites using two different authentication methods and using the results of that authentication process to limit access to content on one of the web sites. Claims 4, 5, 7-13 and 16-20 have been amended to underscore this difference.

§103 Rejection of the Claims

Claims 16-17 were rejected under 35 U.S.C. § 103(a) as being unpatentable over RSA, as applied to claim 4 above, in further view of Network Security Essentials Applications and Standards by Stallings.

Applicant respectfully submits that neither reference describes or suggests authenticating the user to two different web sites using two different authentication methods and using the results of that authentication process to limit access to content on one of the web sites.

In addition, there is no teaching or suggestion in either references to apply private/public key encryption to the one-time password generated by the RSA token.

Reconsideration is respectfully requested.

Claim 13 was rejected under 35 U.S.C. § 103(a) as being unpatentable over RSA, as applied to claim 11 above, in further view of U.S. Patent Application Publication 2001/0045451 to Tan et al. (Tan) in further view of "eToken: The Key to Security for the Internet Age" by Aladdin. Applicant respectfully submits that none of the references describes or suggests authenticating the user to two different web sites using two different authentication methods and using the results of that authentication process to limit access to content on one of the web sites.

Reconsideration is respectfully requested.

CONCLUSION

Applicant respectfully submits that the claims are in condition for allowance, and notification to that effect is earnestly requested. The Examiner is invited to telephone Applicant's attorney at (612) 373-6909 to facilitate prosecution of this application.

If necessary, please charge any additional fees or credit overpayment to Deposit Account No. 19-0743.


Respectfully submitted,

SEAN BRENNAN

By his Representatives,

SCHWEGMAN, LUNDBERG, WOESSNER & KLUTH, P.A.
P.O. Box 2938
Minneapolis, MN 55402
(612) 373-6909

Date March 8, 2006

By 
Thomas F. Brennan
Reg. No. 35,075

CERTIFICATE UNDER 37 CFR 1.8: The undersigned hereby certifies that this correspondence is being deposited with the United States Postal Service with sufficient postage as first class mail, in an envelope addressed to: Mail Stop Amendment, Commissioner of Patents, P.O. Box 1450, Alexandria, VA 22313-1450, on this 8th day of March, 2006.
Thomas F. Brennan

Name


Signature